应用动态安全模型构建信息安全管理体系

摘 要：在实施信息化建设的同时，信息安全的相关工作也在稳步推进。近年来，国内外都在研究如何使用安全框架和分析设计模型，提高信息安全技术和管理方法的最大效能。由此，本文将从信息安全管理和实现具体安全目标的角度出发，对动态安全模型进行分析解读，对如何构建信息安全管理体系进行了梳理和分析，提出完善和改进信息安全管理体系的意见和建议，以开拓一种建立信息系统安全服务体系的新思路。

关键词：信息安全管理体系；管理框架；动态安全模型；管理系统性方法；

中图分类号：TP393　　文献标识码：A

文章编号：1671-0134（2018）03-044-03　　DOI：10.19483/j.cnki.11-4653/n.2018.03.018

文 / 梅春霖

1. 传统信息安全工作中面临的挑战

1.1 重技术、轻管理

各单位对信息系统的安全保护主要围绕业务和技术两个方面。很多单位普遍认为，配备一定的技术防护手段，就能保障系统的安全。但对配套的管理规章制度缺乏执行力度，使信息系统管理单位在安全检查、查漏补缺、系统安全水平测试时，时常出现临时抱佛脚、“应试”“应付”的现象。

1.2 缺乏“改进”和“服务”思维

很多信息系统管理人员仍然抱着信息系统的安全防护，“不出问题”即可的思维。但在信息安全环境日益紧迫的情况下，信息安全工作不能等出了问题才去重视，还应成为信息系统的发展和创新方向。信息安全工作应该是一个动态的持续改进过程，应以动态和改进的“促进服务”思维方式开展信息安全工作。

1.3 信息安全制度未形成体系

各类信息安全工作，关键要素是人。许多信息安全管理单位对安全知识的宣传和培训不足，人员的信息安全防范意识较差。

此外，很多单位缺乏相应的安全方针，制定的管理制度未能成为体系。流程化、规范化的安全管理制度缺失，不能在日常的工作中严格执行，给信息安全工作带来了很多挑战。

1.4 责任管理不到位

许多单位将安全管理员的职责分散到一线的技术运维人员身上，并未设置专职的安全管理员岗位。而普通的系统管理员在进行安全工作时，一方面更关注设备和系统的运行情况，另一方面很难客观地从信息安全的角度出发，评估系统的安全性，准确落实信息安全的规章制度。

此外，随着信息化程度的提高，设备不断增加，运维服务等方面的需求也在不断增加，许多单位开始采用服务外包方式对系统进行管理。而外包服务方的安全水平参差不齐，往往未采取有效的安全措施。

1.5 系统建设中对安全性重视不足

系统建设单位往往对功能性投入较大，却对系统的安全性重视不足，这给后期的运维管理带来了较大的安全隐患。在技术系统运维、管理和规章制度的建设方面，信息安全“缺位”较多，在信息业务和信息安全发生冲突时，信息安全往往要让步于业务。

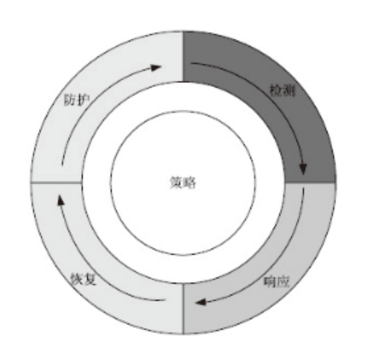
2. 利用动态安全模型建立信息安全体系

要解决现有信息安全管理工作中存在的问题，构建符合信息安全相关规定，适应业务发展的安全体系，首先必须转变思维，将信息安全工作从“严防死守”变为“积极主动”的动态思维。为此，可参照安全评价分析模型，应用管理分析方法和工具进行分析，构建符合信息安全的评价分析体系，从而客观地描述在信息安全工作中所面临的问题、解决方式和完善的环节。

2.1 基于 P2DR2 动态安全模型的信息安全管理框架

在信息安全管理中，人员组织、安全技术及运行操作是三 个主要的支撑体系，P2DR2 动态安全模型的核心思想就是通过对这三个体系进行构建和管理，综合利用技术和管理手段，构建完整的信息安全管理框架。

在信息安全管理框架的构建过程中，需首先确立整体的安全策略，运用各类型手段，了解和评估信息系统



的状态，采用适当的响应和恢复，降低系统的安全风险，减轻因安全事件所产生的风险。

2.1.1 “防护”环节

确保网络层面的结构安全、访问控制、边界完整性检查、恶意代码和入侵防范、网络设备防护。

在主机层面进行入侵防护、恶意代码防护、身份鉴别、系统访问控制、系统资源控制、数据保护、安全特征标记、网络可信路径等安全防护工作。

应用层面包括身份鉴别、访问控制、通信完整性、软件容错、通信保密性、资源控制、剩余信息保护、抗抵赖、安全标记、可信路径。

数据层面包括数据完整性和数据保密性。可以使用多功能防火墙、网络交换和路由设备、入侵检测系统、数据网关、补丁加固系统、防病毒系统、操作系统加固设备、数据库加固设备等各种技术工具和方法，并以安全的配置作为必要的补充。

2.1.2 “监测”环节

为保证信息系统免受安全事件的入侵和破坏，可以采用入侵检测、漏洞扫描、安全审计、防病毒网关、安全管理中心监控等手段。

2.1.3 “响应”环节

安全响应的内容可分为网络和系统安全管理、处理协调和配合机制、安全事件的具体处置、应急响应预案的修订和演练等多项措施，可通过使用安全审计系统、网络运维管理系统，结合专业的技术支持服务和应急响应服务等来实现。

2.1.4 “恢复”环节

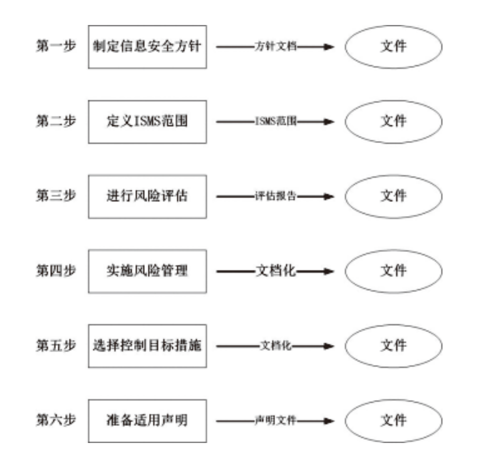
在恢复环节，需要针对系统和数据进行备份和恢复的冗余设计，以保证信息系统可以及时恢复运行。

2.2 利用管理系统性方法进行安全情况评估

利用P2DR2模型构建出适当的信息安全管理框架后，可利用管理系统性方法（ISMS）进行安全情况评估。评估工作以风险信息为基础，将信息安全工作分为建立、实施、运行、监视、评审、保持和改进等若干阶段。

在评估工作中，主要的工作原则包括：

（1）要覆盖信息安全工作的各个环节，并制定相应的规章制度和管理框架。同时，建立相应的风险评价机制，提高信息安全管理的主动性。



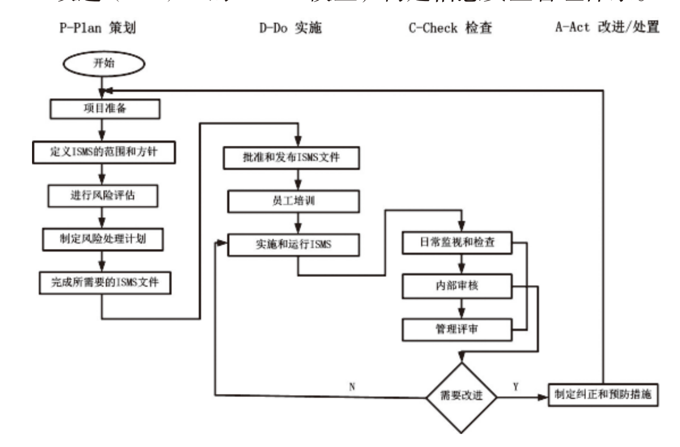
（2）科学分析信息安全管理框架中的各项内容，综合、全面地考虑各环节可能出现的问题。

（3）归档管理各类日志文件和流程化信息。

（4）信息安全的各类信息得到有效反馈。

2.3 使用 PDCA 方法建立信息安全管理体系

在完成了信息安全管理框架的建立和安全情况评估工作后，可以按照“规划（Plan）–实施（Do）–检查（Check）–改进（Act）”的 PDCA 模型，构建信息安全管理体系。



每个阶段的工作内容为：

2.3.1 P（策划）

● 确定信息安全体系的范围和方针

信息安全管理体系应覆盖信息安全工作中的各个阶段，明确界定其作用范围，制定与信息安全环境相关的安全方针，对信息资产进行管理、保护和分配。

● 定义进行风险评估的方法

在进行风险评估的过程中，要选择适当的评估方法，并确定等级准则。一方面，制定风险评估文件，解释所采用的方法、技术和工具，以及应用的业务环境。另一方面，对作用范围内的各类资产和薄弱点进行准确估算，评估出现安全事故时可能造成的影响。

● 对风险进行识别，评估和控制

这一阶段的主要任务是对各类资产的薄弱性、保密性、完整性和可用性缺失时，所造成的影响进行等级划分，从而正确评估风险所造成的损失。同时，还要选择控制风险的方式，以实现风险的控制目标，预防、制止和限制风险，实现恢复控制。

● 统一的管理规划

在信息安全管理体系建立的过程中，需要有统一的规划和明确的任务目标，并能得到相应的管理授权，以便于体系建设工作的正常进行。

2.3.2 D（实施）

● 信息安全管理体系的建立

在这一过程中，主要完成的是进行管理流程、管理规章，管理策划方面的具体运作。通过对风险评估、风险

识别和风险控制的具体分析，分配适当的资源（人员，时间和资金），有针对性地对各类风险制定相应的响应措施。

● 进行管理体系的推广和应用

在信息安全管理体系的推广和应用过程中，应落实各项规章制度，加强对相关人员的安全培训，了解各岗位所处的位置和担负的责任。通过不断加强安全意识，保证各方均能按照要求完成任务。

2.3.3 C（检查）

检查阶段，是 PDCA 循环过程中的关键阶段，是分析运行效果、寻求改进机会的阶段。其目的是及时纠正实施过程中不合理、不充分或难以推进的措施。具体内容包括：

检查实施过程中的错误；能否使各项信息安全管理工作达到预期的结果；接受第三方的安全检查。

评估信息安全管理体系的有效性；收集各类相关的建议和反馈，定期对管理体系进行有效性评审。

确定可风险影响范围和程度，进行风险控制。

对照相关的信息安全管理体系标准，评估技术和管理工作是否适当、是否符合标准以及是否按照预期的目的进行工作。根据需要对内容进行修订。

2.3.4 A（改进）

在改进阶段须对准备实施的方案给出结论，判断信息安全管理体系的可用性和持续性，并对管理体系的推广和颁布做出计划。

2. 4 建立信息安全管理体系时需注意的其他问题

2.4.1 补充 PDCA 中对信息安全管理体系的改进环节

纵观整个通过动态安全模型建立信息安全管理体系的技术和管理等各方面内容，虽然在 PDCA 方法中的 P(策划），D（实施），C（检查）环节均得以较好的进行。但在 A（改进）环节可能缺乏一定的手段和具体措施，不利于对信息安全管理体系的纠正和改进。

因此，在建立新型安全管理体系的改进环节，还需要与实际的运行部门充分进行交流，注意发现问题，提出解决问题的方法和思路，为体系的改进提供基础。

此外，还应通过试点推广、调查反馈以及数据统计等各种手段，获得管理体系实际运行效果的资料，评估其在实际工作中的作用。针对实际效率不高，与业务工作不相符合以致难以推进的内容，予以修订或去除。

2.4.2 建立多元化的信息安全联动机制

在信息安全管理体系的建设和推进过程中，还存在多个层面、多个系统间的多元化的管理协同机制。为此，要以信息安全管理体系为基础，建立多元化的安全联动机制。主要包括监测通报机制、指挥协调机制、信息反馈机制、应急处理机制等。针对各类型的突发事件，还需建立详细可行的安全事件处理流程，按照统一指挥、统一协调、统一接口、统一汇报、统一反馈的原则进行处理，并定期进行安全应急演练。

2.4.3 注重专职安全人员培养机制

在进行信息安全管理体系建设的同时，还应大力加强对专职安全人员的培养机制建设。

加强对信息安全人才的培养。除一线的技术人员要掌握各种安全攻防的技术，具备检测和防范攻击、保护和恢复系统的能力外，安全管理人员还需具备系统安全规划、风险分析、应急响应、安全审计等能力，从机构层面制定信息安全规划，并组织和指挥实施。

2.4.4 建立评价信息安全管理体系的方法

如何对已建立的信息安全管理体系进行绩效衡量，评价体系在实际载体中的运行效果，是在信息安全管理体系的建设和推广过程中需要考虑的问题。

（1）能否满足组织的信息安全管理需求

建立信息安全管理体系的目的是要理顺组织内的安全管理机制，有效应对各类突发事件，提高信息安全的管理水平，增强对各类信息安全风险的管控能力。因此，可对照信息安全工作中的实际需求，逐条进行梳理，并在工作中进行修正，以满足管理工作的现实需要。

（2）采用综合评价的衡量指标

由于信息安全管理体系的建立、推广和使用中不会产生效益，因此，可以根据组织本身的特点，对信息安全管理体系中的各个环节采用综合评价的方法，客观地对信息安全管理体系的效果进行评价。例如，收集取各部门、管理人员、技术人员和使用人员的意见；对比季度或年度的信息安全管理体系运行情况和统计数据; 在运行体系后，安全工作的效率和人员工作量的对比情况等。

（3）建立人员考核和评价体系

人员安全素养的提高与信息安全管理能力、核心防护能力、预防风险能力密切相关。因此，可定期组织对人员的素质进行检查和考核，综合评价安全技术的运用、管理流程的掌控以及协调工作的处理等内容，并根据考核评价情况对问题进行纠正，从而增强组织的运行效率，提高各类人员的职业技能，推动组织的良性发展。媒

参考文献

[1] 谢宗晓 . 信息安全管理体系实施指南 [M]. 北京：中国标准出版社 .2012.

[2] 张泽虹，赵冬梅 . 信息安全管理与风险评估 [M]. 北京：电子工业出版社 .2010.

[3] 王祯学，周安民，方勇等 . 信息系统安全风险估计与控制理论 [M]. 北京：科学出版社 . 2011.

[4] 刘晓敏，许磊 . 信息安全管理体系的定义、功能和构建方法分析 [J]. 北京：信息通信 .2013（1）.

（**作者单位：**新华社通技术局）